UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/533,120	09/19/2005	Bernard Smeets	2380-889	7035

23117 7590 07/10/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
07/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/533,120	SMEETS ET AL.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 47-75 are pending.

2. Amendment filed 05/19/2009 has been received and considered.

Information Disclosure Statement

3. The IDS filed 04/29/2005 was considered by the examiner on 02/09/2009 and a signed copy was included with the action mailed 02/12/2009.

Specification

4. The amendments to the specification have been received and are proper.

Claim Objections

5. The objection to claim 65 has been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 112

6. The rejection of claims 52-54 under the second paragraph of 35 U.S.C. 112 has been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 47, 48, 51-54, 58-64, 66, 67, 69-71, 73 and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins et al. (EP 1081891) in view of Wood et al. (US 20070189534) and further in view of Fujimoto et al. (US 20030033537).

As per claims 47, 66 and 70, Hopkins et al. discloses a storage device for tamper-resistantly storing a secret not accessible over an external circuit interface; a receiver for receiving external data that is external to the tamper-resistant electronic circuit (see paragraph [0032] and [0039] where the external data is the command from the MIF); a processing engine for performing processing at least partly in response to said stored secret to generate an instance of device-specific security data internally confined within said electronic circuit during usage of said device; and electronic circuitry configured to perform a security-related operation in response to said internally confined device-specific security data (see paragraph [0039]).

Hopkins et al. fails to explicitly disclose that the device-specific security data temporal and is generated by performing cryptographic processing on at least partially the stored secret and external data received external to the tamper-resistant electronic circuit wherein the generated temporal instance of device-specific security data depends on a value of said stored secret and a value of said external data and wherein the generated temporal instance of device- specific security data can only be generated as long as external data is available at the receiver.

However, Wood et al. teaches performing cryptographic processing on at least partially secret data and external data to create device-specific security data wherein

the generated instance of security data depends on a value of said stored secret and a value of said external data and wherein the generated instance of security data can only be generated as long as external data is available at the receiver (see paragraphs [0029], [0030] and [0034]) and Fujimoto et al. teaches using a random number to generate a temporary key (see paragraphs [0029] and [0030]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to create temporary device information of Hopkins et al. using a cryptographically generated random number.

Motivation to do so would have been to enhance entropy (see Wood et al. paragraph [0014]) and as recognized by one of ordinary skill in the art to use temporary keys to limit the ability of attackers to break the encryption.

As per claims 48, 67 and 71, the modified Hopkins et al., Wood et al. and Fujimoto et al. system discloses said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication (see Hopkins et al. paragraphs [0030] through [0032]).

As per claims 51-54, 69, 73 and 75, the modified Hopkins et al., Wood et al. and Fujimoto et al. system discloses creating and using triggering data based from cryptographic functions (see Wood et al. paragraphs [0029], [0030], and [0034] and Hopkins et al. paragraphs [0046] through [0053]).

As per claims 58-61, the modified Hopkins et al., Wood et al. and Fujimoto et al. system discloses performing additional cryptographic processing based on the

internally-confined device-specific security data and external data to generate further security data and performing security-related operations in response to said security data where the system is configured to generate and use certain encryption keys (see Hopkins et al. paragraphs [0046] through [0053]).

As per claims 62-64 the modified Hopkins et al., Wood et al. and Fujimoto et al. system discloses generating an internally-confined private key based at least partially on said stored secret (see Hopkins et al. paragraph [0039] as combined with Wood et al. and Fujimoto et al. above) and using the private key and corresponding public key to generate a shared key (see Hopkins et al. paragraphs [0046] through [0053]).

9. Claims 49, 50, 68 and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hopkins et al., Wood et al. and Fujimoto et al. system as applied to claims 47, 66 and 70 above, and further in view of Venkatesan et al. (US 20040001605).

As per claims 49, 50, 68 and 72, the modified Hopkins et al., Wood et al. and Fujimoto et al. system fails to explicitly disclose that the device is configured for producing digital content by marking (by embedding a fingerprint in) said digital content based on the internally-confined temporal device-specific security data.

However, Venkatesan et al. teaches marking produced content with specific security information (see paragraph [0053]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the device specific security information of the modified Hopkins et al., Wood et al. and Fujimoto et al. system to watermark produced content.

Motivation to do so would have been to uniquely identify the content as original (see Venkatesan et al. paragraph [0053]).

10. Claims 55-57 and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hopkins et al., Wood et al. and Fujimoto et al. system as applied to claims 47 and 73 above, and further in view of Beatson (US 20030056100).

As per claims 55-57 and 74, the modified Hopkins et al., Wood et al. and Fujimoto et al. system disclose authenticating a manufacturer and providing information to the manufacturer (see Hopkins paragraphs [0039] through [0042]), but fails to disclose allowing/preventing access to the security information based on an access code.

However, Beatson teaches and access code to prevent/allow access to a device (see Beatson paragraph [0084]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to require an access code to use the device of the modified Hopkins et al., Wood et al. and Fujimoto et al. system.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been to prevent unauthorized access to the security data.

11. Claim 65 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hopkins et al., Wood et al. and Fujimoto et al. system as applied to claim 47 above, in view of Xiao et al. (WO 0077974) and further in view of Matyas, Jr. et al. (US 6687375).

As per claim 65, the modified Hopkins et al., Wood et al. and Fujimoto et al. system fails to disclose generating a chain of keys by hashing a previous key with an identity.

However, Xiao et al. teaches chaining based off values of keys (see page 9 lines 1-10) and Matyas, Jr. et al. teaches creating a key by hashing a key with identity information (see FIG. 4 and column 9 lines 3-17).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to create a chain of user dependent keys in the modified Hopkins et al., Wood et al. and Fujimoto et al. system.

Motivation to do so would have been to create a chain of trust (see Xiao et al. page 9) and to create a user specific key (see Matyas, Jr. et al. column 9 lines 3-17).

Response to Arguments

12. Applicant's arguments (see pages 21-24) with respect to claims 47-75 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Examiner, Art Unit 2437